AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A method of securing access to a piece of equipment, comprising:

one attribution operation supplying a reference datum to an authentication medium;

an acquisition operation obtaining, for every access request formulated by a party requesting access to the piece of equipment, a biometric signature of said party requesting access; ~~and~~

an encryption step storing an encrypted version of at least one authentic biometric signature;

a receiving step receiving and storing a personal identification code attributed to the party authorized to access the piece of equipment;

a matching step matching the stored personal identification code with the stored encrypted version of the at least one authentic biometric signature; and

a verification step verifying, by means of the reference datum, the authenticity of the biometric signature obtained from the party requesting access, further including a prior encryption step, during which [[an]] the encrypted version of the at least one authentic biometric signature belonging to at least one person ~~authorised~~ authorized to access the piece of equipment is created,

wherein the verification step comprises a decryption operation implemented in the authentication medium which includes decrypting, by means of a secret key, the encrypted version of an authentic biometric supplied to said authentication medium as a reference datum during the access request, and

wherein the verification step comprises a comparing operation implemented by secretly comparing the biometric signature obtained from the party requesting access during the access request with the authentic biometric signature that results from the decryption step.

2. (Currently Amended) An authentication medium ~~for implementing the method according to claim 1,~~ comprising an electronic card having at least one decryption module using a secret key, said electronic card performing the following steps:

receiving a reference datum to an authentication medium;

obtaining, for every access request formulated by a party requesting access to the piece of equipment, a biometric signature of said party requesting access;

storing an encrypted version of at least one authentic biometric signature;

receiving and storing a personal identification code attributed to the party authorized to access the piece of equipment;

matching the stored personal identification code with the stored encrypted version of the at least one authentic biometric signature; and

verifying, by means of the reference datum, the authenticity of the biometric signature obtained from the party requesting access, further including a prior encryption step, during which the encrypted version of the at least one authentic

biometric signature belonging to at least one person authorized to access the piece of equipment is created,

wherein the verification comprises a decryption operation implemented in the authentication medium which includes decrypting, by means of a secret key, the encrypted version of an authentic biometric supplied to said authentication medium as a reference datum during the access request, and

wherein the verification comprises a comparing operation implemented by secretly comparing the biometric signature obtained from the party requesting access during the access request with the authentic biometric signature that results from the decryption step.

3. (Currently Amended) ~~An~~ The authentication medium according to claim 2, further comprising a comparison module.

4. (Currently Amended) ~~An~~ The authentication medium according to claim 2, further comprising an encryption module.

5. (Currently Amended) A device for securing access to a piece of equipment, comprising:

an authentication medium which is supplied with a reference datum;

a sensor obtaining, during every access request formulated by a party requesting access to the piece of equipment, a biometric signature of said party requesting access; ~~and~~

a computer storing in its memory an encrypted version of an authentic biometric signature and a personal identification code attributed to the party authorized to access the piece of equipment, and matching the stored personal identification code with the stored encrypted version of the authentic biometric signature; and

a controller included in the authentication medium and selectively ~~authorising~~ authorizing the party requesting access to access the piece of equipment in accordance with the result of a verification of the authenticity of the biometric signature of the party requesting access, the controller ~~comprises~~ comprising a decryption module and a comparison module, wherein the reference datum supplied to the authentication medium comprises [[an]] the encrypted version of [[an]] the authentic biometric signature corresponding to the personal identification code ~~allegedly~~ attributed to the party requesting access, wherein the decryption module uses a secret key by means of which it secretly reconstructs, upon each access request, the authentic biometric signature from its encrypted version, and wherein the comparison module secretly compares the biometric signature obtained from the party requesting access with the reconstructed authentic biometric signature, and supplies a comparison result that constitutes the result of the verification.

6. (Currently Amended) ~~A security~~ The device according to claim 5, wherein the authentication medium is a card, equipped with a memory that cannot be read from outside, in which the secret key is stored.

7. (Currently Amended) ~~A security~~ The device according to claim 5, ~~further comprising~~ wherein at least one computer ~~that~~ makes up at least a part of the equipment to which the access is secured.

8. (Currently Amended) ~~A security~~ The device according to claim 7, wherein the at least one computer contains in its memory a plurality of personal identification codes attributed to a corresponding plurality of persons ~~authorised~~ authorized to access the equipment and associated with a corresponding plurality of encrypted authentic biometric signatures for these ~~authorised~~ authorized persons, and wherein the at least one computer delivers to the ~~identification~~ authentication medium, when receiving an access request, the encrypted authentic biometric signature that corresponds to the personal identification code supplied by the party requesting access, such that a single authentication medium provides several persons with secure access to the computer.

9. (Currently Amended) ~~A security~~ The device according to claim 5, further comprising an encryption module that delivers an encrypted version of an authentic biometric signature supplied in plain form by the sensor in response to an encryption command.

10. (Currently Amended) ~~A security~~ The device according to claim 9, wherein the secret key is a private key with a matching public key, and wherein the encryption module is included in the computer and uses the public key.

11. (Currently Amended) ~~An~~ The authentication medium according to claim 3, further comprising an encryption module.

12. (Currently Amended) ~~A security~~ The device according to claim 6, further comprising at least one computer that makes up at least a part of the equipment to which the access is secured.

13. (Currently Amended) ~~A security~~ The device according to claim 6, further comprising an encryption module that delivers an encrypted version of an authentic biometric signature supplied in plain form by the sensor in response to an encryption command.

14. (Currently Amended) ~~A security~~ The device according to claim 7, further comprising an encryption module that delivers an encrypted version of an authentic biometric signature supplied in plain form by the sensor in response to an encryption command.

15. (Currently Amended) ~~A security~~ The device according to claim 8, further comprising an encryption module that delivers an encrypted version of an authentic biometric signature supplied in plain form by the sensor in response to an encryption command.